SKRIPSI

ANALISIS RESIKO KERENTANAN KOMUNIKASI DATA PADA PERANGKAT PENDUKUNG INDUSTRI 4.0

Oleh:

Damara Putra Pratama

NIM: 04215034

PROGRAM STUDI SISTEM INFORMASI

FAKULTAS ILMU KOMPUTER

UNIVERSITAS NAROTAMA

SURABAYA

2019

SKRIPSI

ANALISIS RESIKO KERENTANAN KOMUNIKASI DATA PADA PERANGKAT PENDUKUNG INDUSTRI 4.0

HALAMAN JUDUL

Disusun Oleh:

DAMARA PUTRA PRATAMA
NIM: 04215034

Diajukan guna memenuhi persyaratan
untuk memperoleh gelar Sarjana Komputer (S.Kom)
pada Program Studi Sistem Informasi
Fakultas Ilmu Komputer
Universitas Narotama Surabaya

Surabaya, Agustus 2019

Menyetujui
Dosen Pembimbing

Made Kamisutara, ST., M.Kom
NIDN: 0706027501

ANALISIS RESIKO KERENTANAN KOMUNIKASI DATA PADA

PERANGKAT PENDUKUNG INDUSTRI 4.0

DAMARA PUTRA PRATAMA

NIM: 04215034

Dipertahankan di depan Penguji Skripsi
Program Studi Sistem Informasi
Fakultas Ilmu Komputer
Universitas Narotama Surabaya
Tanggal : 28 Juli 2019

Penguji,

1. **Lukman Junaedi, S.T., M.Kom**
   NIDN : 0711018101

2. **Rangsang Purnama, S.Kom., M.Kom**
   NIDN : 0711087301

3. **Made Kamisutara, ST., M.Kom**
   NIDN: 0706027501

Ketua Program Studi,

Immah Inayati, S.Kom., M.Kom., MBA
NIDN : 0714128502

Fakultas Ilmu Komputer
Dekan,

Aryo Nugroho, S.T., S.Kom., M.T
NIDN : 0721077001

SURAT PERNYATAAN

Dengan ini saya menyatakan bahwa dalam Skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat Karya/Pendapat yang pernah ditulis oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam Daftar Acuan/Daftar Pustaka.

Apabila ditemukan suatu Jiplakan/Plagiat maka saya bersedia menerima akibat berupa sanksi Akademis dan sanksi lain yang diberikan oleh yang berwenang sesuai ketentuan peraturan dan perundang-undangan yang berlaku.

Surabaya, 28 Juli 2019

Penulis

Damara Putra Pratama

NIM: 04215034

ABSTRAK

Dimulainya era industri 4.0 membuat para pelaku industri mulai sadar akan pentingnya peranan IT dalam perusahaan mereka,dengan melibatkan IT dalam beberapa kegiatan di perusahaan mereka semuanya akan menjadi lebih praktis dan taktis. Namun dengan dimulainya era industri 4.0 ini juga membuat ancaman baru pada perusahaan mereka dimana perangkat-perangkat pendukung IT yang banyak varian dan model dari berbagai vendor sehingga para pelaku bisnis harus hati-hati dan teliti karena ada beberapa perangkat pendukung yang kerap kali menjadi sasaran tindak kejahatan siber, salah satu faktornya adalah mudahnya perangkat tersebut di eksploitasi dari segi informasi maupun secara keseluruhan dengan mengontrol perangkatnya.

Dari munculnya permasalahan terkait isu kerentanan pada perangkat-perangkat pendukung industri 4.0 dibuatnya penelitian untuk bagaimana mendeteksi dan menilai tingkat kerentanan pada sebuah perangkat pendukung industri 4.0 dengan menggunakan metode Information Gathering dan Vulnerability Metrics dalam mencari dan menilai kerentanan dari perangkat yang akan diuji.

Dengan melakukan test dengan mengumpulkan informasi terkait port berapa saja yang terbuka dalam sebuah perangkat lalu berapa banyak Common Vulnerability Exposure(CVE), dan Attack Surface dari perangkat-perangkat yang telah diuji akan mengeluarkan laporan terkait positif atau negative perangkat tersebut bisa diesploitasi

Kata Kunci : Industri 4.0 , Analisis Resiko Kerentanan , Information Gathering, Vulnerability Metrics, Hacking, Open Port, CVE, CVSS.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

KESIMPULAN

Kesimpulan yang diperoleh dari penelitian ini adalah memberikan hasil output berupa device-device apa saja yang bisa dieksploitasi menurut perhitungan jumlah Common Vulnerability Exposure (CVE), Attack Surface, dan Web Application yang berjalan. Selain itu port yang terbuka juga mempengaruhi hasil dari penilaian dari penelitian ini. bagaimana masih banyaknya perangkat-perangkat pendukung industri 4.0 yang masih sangat mungkin di retas oleh pelaku kejahatan siber, oleh karena itu perlu adanya kesadaran terhadap keamanan informasi oleh para pelaku industri 4.0 ini supaya perangkat-perangkat yang meraeka gunakan nantinya tidak dijadikan sasaran dari pelaku kejahatan siber. Training dan update informasi terkait keamanan sistem dan perangkat juga diperlukan dan rutin dilakukan agar mereka mengerti bahaya apa saja yang mengancam perangkat-perangkat yang mereka gunakan.

DAFTAR PUSTAKA

[1] A. Reno, "Analisis dampak industri 4.0 terhadap sistem pengawasan ketenaganukliran di indonesia," pp. 47–54, 2018.

[2] Supanto, "PERKEMBANGAN KEJAHATAN TEKNOLOGI INFORMASI (CYBER CRIME) DAN ANTISIPASINYA DENGAN PENAL POLICY," vol. 5, no. 1, 2016.

[3] J. Unp, S. Resmi, and U. Negeri, "Permasalahan Hukum dalam Menanggulangi Cyber Crime di Indonesia," no. August 2017, 2018.

[4] D. De Roure, S. Cannady, R. Mantilla Montalvo, R. Nicolescu, M. Huth, and P. Radanliev, "Analysing IoT cyber risk for estimating IoT cyber insurance." 2019.

[5] A. Fajaryanto, U. M. Ponorogo, T. Dirgahayu, U. I. Indonesia, Y. Prayudi, and U. I. Indonesia, "Penerapan Metode ISSAF dan OWASP versi 4 Untuk Uji Kerentanan Web Server," no. January, 2015.

[6] U. T. Departemen Teknik Informatika, "Analisis Risiko Teknologi Informasi Berbasis Risk Management Menggunakan ISO 31000," vol. 2, no. 2, pp. 1–8, 2015.

[7] A. M. R. Wajong, "Kerentanan Di Jaringan Komputer Pada Umumnya," vol. 3, no. 9, pp. 474–481.

[8] J. R. Treurniet, "An Overview of Passive Information Gathering Techniques for

Network Security," no. May, p. 44, 2004.

[9] "Shodan.io." [Online]. Available: https://id.wikipedia.org/wiki/Shodan_(situs_web).

[10] P. W. Widya, R. M. Ijtihadie, and B. A. Pratomo, "Rancang Bangun Layanan Platform as a Service (PAAS) untuk Mendukung Sistem Multi-Tenancy Pengembangan Aplikasi Berbasis Komputasi Awan," *J. Tek. Pomtits*, vol. 2, no. 1, pp. 1–6, 2013.

[11] Mitre Corporation, "About CVE." [Online]. Available: https://cve.mitre.org/about/index.html.

[12] "Nmap." [Online]. Available: https://nmap.org/man/id/index.html.

[13] F. Maria Rosario B, Yovi Pratama, "Penerapan Web Scraping Pada Website Company Profile," *Kntia*, vol. 4, no. 4, pp. 37–43, 2017.

[14] P. Studi, T. Elektro, S. Teknik, and E. Dan, "STUDI TINGKAT KEAMANAN PASSWORD PADA DATA , EMAIL , DAN APLIKASI Disusun sebagai :," no. November, 2007.